Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2015, Article ID 206954, 7 pages
http://dx.doi.org/10.1155/2015/206954

Research Article

Optimal Jamming Attack Scheduling in Networked Sensing and Control Systems

Lifu Zhang,[1] Heng Zhang,[2] Cunhua Li,[2] and Buxi Ni[1]

[1] *Wenzhou Vocational & Technical College, Wenzhou 325000, China*
[2] *Huaihai Institute of Technology, Lianyungang 222000, China*

Correspondence should be addressed to Heng Zhang; ezhangheng@gmail.com

Received 8 June 2015; Revised 19 August 2015; Accepted 16 September 2015

Academic Editor: Jianping He

This paper investigates the optimal jamming attack scheduling in Networked Sensing and Control Systems (NSCS). From viewpoint of the attacker, we formulate an optimization problem which maximizes the Linear Quadratic Gaussian (LQG) control cost with attacking energy constraint in a finite time horizon. For two special cases, we obtain that the optimal jamming attack schedule is to consecutively attack in the given time horizon. For the general case, we propose an algorithm to find the optimal schedules. Finally, we study the effectiveness of our proposed attack strategies on our established semiphysical testbed.

1. Introduction

Networked Sensing and Control Systems (NSCS) are control systems wherein physical elements, that is, plants, sensors, controllers, and actuators, are connected via wireless communication networks. NSCS have a wide range of applications in factory automation, unmanned aerial vehicles, remote surgery, intelligent transportation, smart grid, smart building, and so forth [1–5]. The essential characteristic of NSCS is that the physical elements and cyberspace are tightly integrated to carry out various jobs [6–8]. However, NSCS are vulnerable to an increasing number of malicious cyber attacks [9]. For example, an Iranian nuclear facility was attacked by "stuxnet" in 2010 and cannot operate normally in a long time since more than 60% of centrifugal control systems were destroyed [10].

In the past few years, several literatures have been focused on evaluating the effect of cyber attacks, for example, Denial-of-Service (DoS) attacks [11, 12], replay attacks [13, 14], and false data injection attacks [15, 16], on NSCS. Among these attacks, DoS attack is the most accomplishable one and can result in serious consequences [11]. Thus, it has been widely studied recently. In order to block the communication between system elements, DoS attacker can interfere with the radio frequencies on the communication channels [17]. In fact, jamming is a typical mode of DoS attack [18].

LQG control cost, which is used to synthetically consider the cost of system states and control, is an important performance in NSCS. Some researches have put emphasis on the security of LQG control under jamming attack [11, 19, 20]. Amin et al. study the optimal controller which minimize the LQG cost with safety and energy constraints when a jamming attacker takes identical independent distributed jamming actions [11]. They present semidefinite programming to solve this problem. Gupta et al. design an optimal controller to defense the intelligent jamming attack with limited actions [19]. Shisheh Foroush and Martinez propose an event-trigger control law which can prevent the periodic jamming attack with energy constraint [20]. The commonality of these works is that they all focus on the design of defense strategies under given attack patterns. However, our work stands in the viewpoint of attacker and finds the optimal attack schedules to maximize the control performance. This is of equal importance as one can provide effective defensive policies only when he grasps the attack strategies.

The goal of this paper is to design an optimal offline jamming schedule, which can maximize the attack effect on the NSCS. Specifically, in our scenario, one sensor observes the states of plant and sends the measurements to a remote estimator via a wireless channel. The attacker has a limited energy budget in the given finite time horizon. He has to decide

whether or not to jam the channel from sensor to estimator at each time. The main contributions of this paper which distinguish it from the related literatures are summarized as follows:

(1) We formulate a jamming attack scheduling problem and look for the optimal jamming schedule that maximizes the LQG cost with energy constraint in a given finite time horizon.

(2) We present the close form of the optimal jamming schedule for two special cases and provide an algorithm to search the optimal schedules for the general case.

(3) We study the effectiveness of proposed jamming schedules on the established semiphysical testbed.

The remainder of the paper is organized as follows. In Section 2, we formulate the problem. In Section 3, we study the system performance under given attack schedule. In Section 4, we present the optimal jamming attack schedules for special cases and provide an algorithm to search the optimal attack schedules for the general case. In Section 5, we demonstrate the effectiveness of proposed optimal jamming schedules on the semiphysical testbed. Finally, Section 6 concludes the paper.

Notations. $\mathbb{E}[X]$ is the mean of random variable X, and $\mathbb{E}[X \mid Y]$ is the mean of random variable X conditioned on Y, respectively. $\mathrm{tr}(\cdot)$ represents the trace of matrix. $X \preceq Y$ means that $Y - X$ is nonnegative-definite; that is, $Y - X \succeq 0$.

2. Problem Formulation

2.1. System Architecture. Consider the following linear time-invariant system (Figure 1):

$$\begin{aligned} x_{t+1} &= Ax_t + u_t + w_t, \\ y_t &= Cx_t + v_t, \end{aligned} \tag{1}$$

where $x_t \in \mathbb{R}^{n_x}$ is the state of plant at time t, $y_t \in \mathbb{R}^{n_y}$ is the measurement from sensor, and w_t and v_t are uncorrelated zero mean Gaussian white noises with covariance Σ_w and Σ_v, respectively. The pair (A, C) is assumed to be observable and $(A, \Sigma_w^{1/2})$ is controllable.

In our scenario, the sensor observes the plant and gets the measurements y_t. According to these measurements, it preestimates the state x_t and obtains the minimum mean squared error (MMSE) estimate; that is, $\widehat{x}_t^s = \mathbb{E}[x_t \mid y_1, \ldots, y_t]$. Then the sensor sends these estimates to a remote estimator through a wireless channel. The controller then generates a control packet u_t based on the received estimates and sends the control packet to the actuator through another dependable channel.

Let θ_t be the indicator function whether the packet $\widehat{x}_t^s$ is received or not by the estimator; that is,

$$\theta_t = \begin{cases} 1, & \text{if } \widehat{x}_t^s \text{ is received by the estimator;} \\ 0, & \text{otherwise.} \end{cases} \tag{2}$$

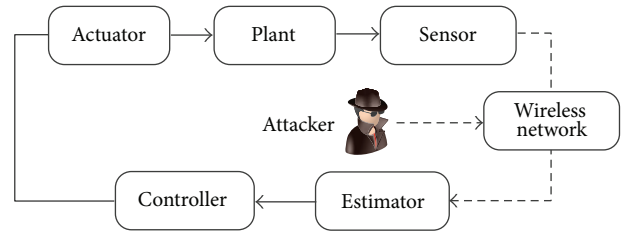


Figure 1: System architecture.

Denote $\mathscr{D}_t$ by all the data received by estimator until time t; that is,

$$\mathscr{D}_t = \{\theta_1, \theta_2, \ldots, \theta_t, \theta_1 \widehat{x}_1^s, \theta_2 \widehat{x}_2^s, \ldots, \theta_t \widehat{x}_t^s\}. \tag{3}$$

Let $\widehat{x}_t$ be the minimum mean square error (MMSE) estimate in the estimator at time t; that is,

$$\widehat{x}_t = \mathbb{E}\left[x_t \mid \mathscr{D}_t\right]. \tag{4}$$

The corresponding error covariance is

$$P_t = \mathbb{E}\left[\left(x_t - \widehat{x}_t\right)\left(x_t - \widehat{x}_t\right)' \mid \mathscr{D}_t\right]. \tag{5}$$

Similar to [21], we have

$$\widehat{x}_t = \begin{cases} \widehat{x}_t^s, & \text{if } \theta_t = 1; \\ A\widehat{x}_{t-1}^s + Bu_{t-1}, & \text{otherwise.} \end{cases} \tag{6}$$

In order to minimize the LQG cost function

$$J = \sum_{t=0}^{T-1} \mathbb{E}\left[x_t' Q x_t + u_t' R u_t\right] + x_T' Q x_T \tag{7}$$

in the finite time horizon $[1, T]$, where $Q \succeq 0$ and $R \succ 0$ are two weighting matrices and the expectation is taken over $\{w_k\}$, we exploit a linear static feedback controller of the form $u_k = L\widehat{x}_k$. It is assumed that the system is unaware of the existence of attacker.

2.2. Attack Model. In our scenario, there is an attacker who wishes to deteriorate the control performance by jamming the sensor-to-estimator wireless channel. It is assumed that the attacker has a limited energy budget; that is, he can attack n times at most in the time horizon $[1, T]$ [22]. The attacker has to decide whether to attack or not at each sampling time in order to achieve his aim. Let γ_t be the attack decision variable at time t; that is,

$$\gamma_t = \begin{cases} 1, & \text{if attacker jams the wireless channel;} \\ 0, & \text{otherwise.} \end{cases} \tag{8}$$

Similar to [18], we assume that the attack action is successful with probability α, and packet drop variables under attack are independent.

Specifically, from the viewpoint of attacker, he aims to maximize the cost function with energy constraint which is as follows.

Problem 1. Consider

$$\begin{aligned} \max_{\gamma\in\Theta} \quad & \mathbb{E}\left[J\left(\gamma\right)\right] \\ \text{s.t.} \quad & \sum_{t=1}^{T}\gamma_t \le n, \end{aligned} \tag{9}$$

where $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_T)$ is the attack schedule on the finite time horizon $[1, T]$ and $\Theta = \{\gamma \mid \gamma_t \in \{0, 1\},\ t = 1, 2, \ldots, T\}$ is the attack schedule space.

3. Preliminaries

In this section, we present some properties of the estimate at the estimator side and the control performance of plant under a jamming attack.

3.1. State Estimation under Jamming Attack. From standard Kalman filter, the estimate and corresponding error covariance at the sensor side can be calculated as follows:

$$\begin{aligned} \widehat{x}^s_{t|t-1} &= A\widehat{x}^s_{t-1} + u_{t-1}, \\ P^s_{t|t-1} &= AP^s_{t-1}A' + \Sigma_w, \\ K^s_t &= P^s_{t|t-1}C'\left[CP^s_{t|t-1}C' + \Sigma_v\right]^{-1}, \\ \widehat{x}^s_t &= A\widehat{x}^s_{t-1} + K^s_t\left(y_t - C\widehat{x}^s_{t|t-1}\right), \\ P^s_t &= \left(I - K^s_tC\right)P^s_{t|t-1}, \end{aligned} \tag{10}$$

where the initial state is $\widehat{x}_0 = 0$, and $P^s_0 = \Pi_0$. From [23], we can see that the error covariance P^s_t converges exponentially to its steady-state value $\overline{P}$. Thus, we assume that $\Pi_0 = \overline{P}$. It can be seen that $P^s_t = \overline{P}$ for all $t \in [1, T]$.

Define functions h, h^t as $h(X) \triangleq AXA' + \Sigma_w$ and $h^t(X) \triangleq \underbrace{h \circ h \circ \cdots \circ h}_{t \text{ times}}(X)$.

From [23], the following result holds.

Lemma 2. *The function h has the following property:*

$$\overline{P} \preceq h\left(\overline{P}\right) \preceq h^2\left(\overline{P}\right) \preceq \cdots \preceq h^t\left(\overline{P}\right) \preceq \cdots, \quad \forall t \in \mathbb{Z}^+. \tag{11}$$

From [22], we can obtain the estimate $\widehat{x}_t$ and error covariance P_t at estimator side as follows:

$$\left(\widehat{x}_t, P_t\right) = \begin{cases} \left(A\widehat{x}_{t-1} + u_{t-1}, h\left(P_{t-1}\right)\right), & \text{if } \gamma_t = 1,\ \theta_t = 1, \\ \left(\widehat{x}^s_t, \overline{P}\right), & \text{otherwise.} \end{cases} \tag{12}$$

Define attack sequence $(k_1, k_2, \ldots, k_s)$ as the attack schedules which has the following form:

$$\left(0, \ldots, 0, \underbrace{1, \ldots, 1}_{k_1 \text{ times}}, 0, \ldots, 0, \underbrace{1, \ldots, 1}_{k_2 \text{ times}}, 0, \ldots, 0, \underbrace{1, \ldots, 1}_{k_s \text{ times}}, 0, \ldots, 0\right). \tag{13}$$

Similar to [18, 22], one can get the following result.

Lemma 3. *Let $E(k_1 \otimes k_2 \otimes \cdots \otimes k_s)$ be the average expected error covariance in time horizon $[1, T]$ under attack sequence $(k_1, k_2, \ldots, k_s)$ at estimator side, and let $E(k)$ be the average expected error covariance under attack sequence (k). The following statements are true:*

(1) *$E(k_1) \preceq E(k_2)$, where $k_1 < k_2$.*

(2) *$E(k_1 \otimes k_2 \otimes \cdots \otimes k_s) \preceq E(k)$, where $k = k_1 + k_2 + \cdots + k_s$.*

(3) *$E(k_1 \otimes k_2) \preceq E(l_1 \otimes l_2)$, where $k_1 + k_2 = l_1 + l_2$ and $\max\{k_1, k_2, l_1, l_2\}$ is l_1 or l_2.*

From Lemma 3, we can see that grouping together as much as possible can lead to maximal average error covariance.

3.2. Control Performance under Jamming Attack. In order to find the optimal offline jamming attack scheduling, we have to study the control performance when the attack schedule is given.

According to [5, 24], one can obtain the following result.

Lemma 4. *The LQG control cost function under a given attack schedule γ can be calculated as follows:*

$$\begin{aligned} J\left(\gamma\right) = {} & \operatorname{tr}\left(S_0P_0\right) + \sum_{t=0}^{T-1}\operatorname{tr}\left(S_{t+1}\Sigma_w\right) \\ & + \sum_{t=0}^{T-1}\operatorname{tr}\left[\left(A'S_{t+1}A + Q - S_t\right)E_\gamma\left(P_t\right)\right], \end{aligned} \tag{14}$$

where S_t can be computed from the following recursive equation:

$$S_t = A'S_{t+1}A + Q - A'S_{t+1}\left(S_{t+1} + R\right)^{-1}S_{t+1}A, \quad t = 0, 1, \ldots, T-1. \tag{15}$$

In fact, (15) converges quickly to a steady state. Thus, if $T \to \infty$, one can see that

$$S = A'SA + Q - A'S\left(S + R\right)^{-1}SA, \tag{16}$$

where $S = \lim_{T\to\infty}S_T$. In practice, we often choose $u_t = L\widehat{x}_t$ with control gain $L = -(S + R)^{-1}SA$ as the optimal static state feedback controller to maximize the cost $J_\infty = \lim_{T\to\infty}J$.

In our scenario, we assume that the system has reached steady state; that is, $S_0 = S$, and $P_0 = \overline{P}$. Then (14) can be rewritten as

$$J(\gamma) = J_c + J_e, \tag{17}$$

where

$$\begin{aligned} J_c &= \operatorname{tr}\left(S\overline{P}\right) + N \cdot \operatorname{tr}\left(S\Sigma_w\right), \\ J_e &= \sum_{t=0}^{T-1} \operatorname{tr}\left[\left(A'SA + Q - S\right)\mathbb{E}_\gamma\left(P_t\right)\right]. \end{aligned} \tag{18}$$

It can be seen that J_c and J_e are the constant part and varying part of (17), respectively. Thus, we only have to study the optimal jamming attack schedule which maximizes J_e which is as follows.

Problem 5. Consider

$$\begin{aligned} \max_{\gamma\in\Theta} \quad & \mathbb{E}\left[J_e(\gamma)\right] \\ \text{s.t.} \quad & \sum_{t=1}^{T} \gamma_t \le n. \end{aligned} \tag{19}$$

4. Optimal Jamming Attack Schedules

In this section, we firstly study the jamming schedules against LQG control for two special cases and present the close form of optimal schedules. Then we investigate the attack strategies for the general case.

4.1. Case I: $R = 0$. When $R = 0$, it can be seen that the LQG cost function becomes

$$J = \sum_{t=0}^{T} \mathbb{E}\left[x_t' Q x_t\right]. \tag{20}$$

From Lemma 4, we can obtain the following conclusion.

Theorem 6. *If $R = 0$, the optimal state feedback controller is $u_t = L\widehat{x}_t = -A\widehat{x}_t$, and the corresponding LQG cost function under attack schedule γ is*

$$J = J_c + J_e, \tag{21}$$

where

$$\begin{aligned} J_c &= \operatorname{tr}\left(Q\overline{P}\right) + N \cdot \operatorname{tr}\left(Q\Sigma_w\right), \\ J_e &= \sum_{t=0}^{T-1} \operatorname{tr}\left[A'QA\mathbb{E}_\gamma\left(P_t\right)\right]. \end{aligned} \tag{22}$$

According to Theorem 6, we can see that the attacker only needs to maximize $\mathbb{E}[J_e]$. Since $A'QA \succeq 0$, one can obtain that $\max_\gamma \mathbb{E}[J_e]$ is equivalent to $\max_\gamma \mathbb{E}[\sum_{t=0}^{N-1} P_t(\gamma)]$. Thus, from viewpoint of attacker, we only have to solve the following problem.

Problem 7. Consider

$$\begin{aligned} \max_{\gamma\in\Theta} \quad & \mathbb{E}\left[\sum_{t=0}^{N-1} P_t(\gamma)\right] \\ \text{s.t.} \quad & \sum_{t=1}^{T} \gamma_t \le n. \end{aligned} \tag{23}$$

From [18, 22], Problem 7 can be easily solved by the following theorem.

Theorem 8. *When $R = 0$, the optimal attack schedules are any consecutive attack n times in time horizon $[1, T]$, and the corresponding expected LQG cost function is*

$$\mathbb{E}(J) = J_c + J_e^{\max}, \tag{24}$$

where

$$J_e^{\max} = \sum_{i=1}^{T} \operatorname{tr}\left[g_i\left(\overline{P}\right)\right] + (T - n\alpha)\operatorname{tr}\left[M\overline{P}\right], \tag{25}$$

with $M = A'QA$ and $g_i(\overline{P}) = Mh^i(\overline{P})$.

4.2. Case II: $S_0 = S$. Define $\overline{M} = A'SA + Q - S$, and $\overline{g}_i(\overline{P}) = \overline{M}h^i(\overline{P})$, $i = 1, 2, \ldots$. Then we have following lemma.

Lemma 9. *The function $\overline{g}$ has the following property:*

$$\overline{g}_1\left(\overline{P}\right) \preceq \overline{g}_2\left(\overline{P}\right) \preceq \cdots \preceq \overline{g}_i\left(\overline{P}\right) \preceq \cdots. \tag{26}$$

According to Section 3.2, the objective of Problem 1 is equivalent to $\max_\gamma \mathbb{E}[\sum_{t=0}^{N-1} P_t(\gamma)]$. Thus, from the viewpoint of attacker, we only have to solve Problem 7 for the case $S_0 = S$.

From Lemma 9 and Theorem 3.1 in [22], we can solve this problem by the following theorem.

Theorem 10. *When $S_0 = S$, the optimal attack schedules are any consecutive attack n times in time horizon $[1, T]$, and the corresponding expected LQG cost function is*

$$\mathbb{E}(J) = J_c + J_e^{\max}, \tag{27}$$

where

$$J_e^{\max} = \sum_{i=1}^{T} \operatorname{tr}\left[\overline{g}_i\left(\overline{P}\right)\right] + (T - n\alpha)\operatorname{tr}\left[\overline{M} \cdot \overline{P}\right]. \tag{28}$$

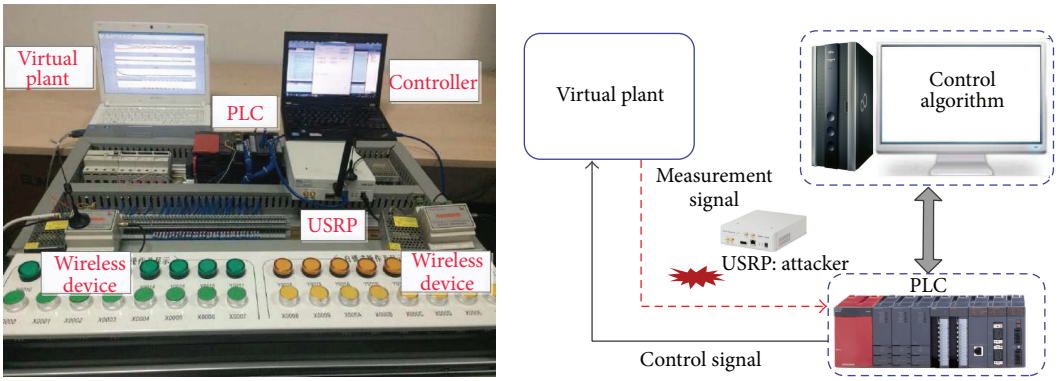
4.3. General Case Study. For the general case, it is difficult to obtain a close form of optimal attack schedule. Attacker can find the optimal jamming schedule by exhaustion method which is given in Algorithm 1. Since this schedule can be computed before the attack action begins, the computation of our proposed algorithm will not cost too much.

5. Simulation

5.1. Testbed. There are three types testbeds for simulation of NSCS security, that is, software simulation testbeds, physical

(1) Process begins;
(2) Input: $H_{\text{time}} = T$; $\Pi_0 = \overline{P}$; $J^* = 0$;
(3) **for** $\gamma_1 + \gamma_2 + \cdots + \gamma_T = n$ **do**
(4) Compute LQG cost (14) under attack schedule γ, that is $J = J(\gamma)$
(5) **if** $J > J^*$ **then**
(6) $J^* = J$, and $\gamma^* = (\gamma_1, \gamma_2, \ldots, \gamma_T)$
(7) **end if**
(8) **end for**
(9) Output: optimal attack schedule γ^*, and corresponding cost J^*.

Algorithm 1: Optimal offline attack schedule.



(a) The physical structure (b) The schematic diagram

Figure 2: The structure of semiphysical testbed.

simulation testbeds, and semiphysical simulation testbeds. The software simulation testbeds cannot fully simulate the real environment. The physical simulation testbeds can employ the same experimental equipment with the real world to construct the security test platform. However, they need long cycle of construction and great cost. Fortunately, semiphysical simulation testbeds are the good choice for NSCS security since they can simulate the real working environment and save the cost. Thus, we choose a semiphysical simulation testbed to study the effectiveness of our proposed attack strategy.

Our semiphysical simulation testbed is composed of virtual plant, physical controller, and communication network. Figure 2 shows the system architecture. In our testbed, real-time system states of the virtual plant are sent to the PLC through a wireless network. After reading the system states, the controller calculates the control data and writes them back to the PLC. Then the control data are sent back to the virtual plant via a wired channel.

We build an inverted pendulum control system for experiments, which is based on the system presented in [5]. The parameters are given as follows:

$$A = \begin{pmatrix} 1.001 & 0.005 & 0.000 & 0.000 \\ 0.350 & 1.001 & -0.135 & 0.000 \\ -0.001 & 0.000 & 1.001 & 0.005 \\ -0.375 & -0.001 & 0.590 & 1.001 \end{pmatrix},$$

$$B = \begin{pmatrix} 0.001 \\ 0.540 \\ -0.002 \\ -1.066 \end{pmatrix},$$

$$\Sigma_w = qq', \quad q = \begin{pmatrix} 0.003 \\ 1.000 \\ -0.005 \\ -2.150 \end{pmatrix},$$

$$Q = \begin{pmatrix} 5 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{29}$$

We employ USRP N210 to simulate jamming attack on the wireless channel from sensor to controller. USRP is a universal software radio peripheral that can send and receive radio signal. We use the software GNU Radio in Ubuntu to manipulate the USRP. The frequency spectrum analyzer is adopted to detect the central frequency and waveform of transmission signals. Then we adapt the parameters on GNU Radio to configure the USRP. Experimental parameters are

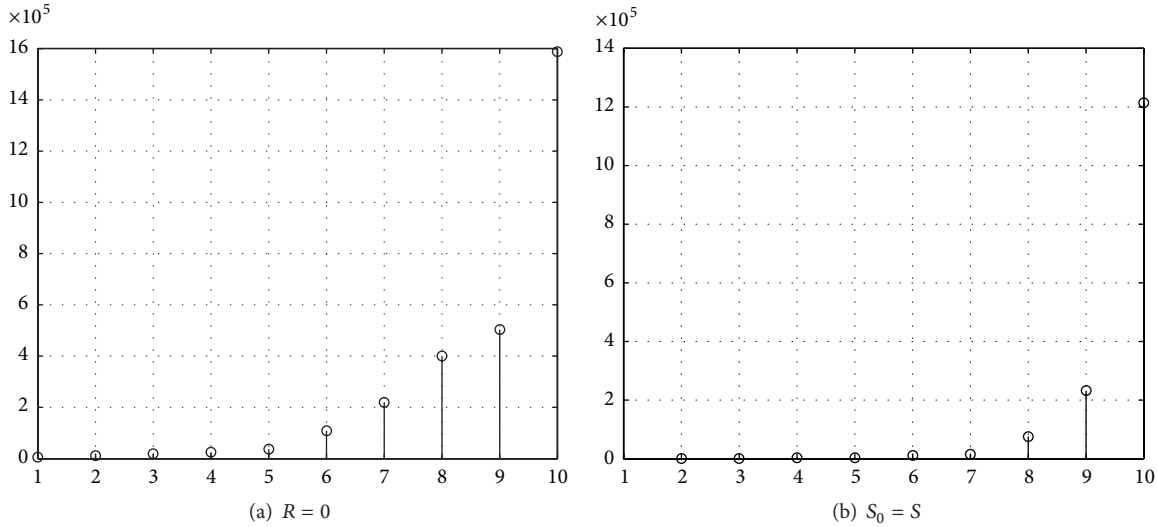


Figure 3: Compare the cost J under different attack strategies. The lateral axis is the mark number of attack strategy. Attack strategy 10 is the consecutive attack strategy.

Table 1: Attack schedules in our experiment.

Mark number	1	2	3	4	5
Attack sequence	No attack	(1, 2, 3, 4)	(6, 3, 1)	(4, 4, 2)	(5, 5)
Mark number	6	7	8	9	10
Attack sequence	(4, 6)	(7, 3)	(8, 2)	(9, 1)	(10)

set as follows: center frequency is 433 MHz; waveform is saw tooth; jamming power is 16 dB and jamming signal frequency is 10k; bandwidth is 20 MHz.

We verify the proposed optimal offline attack strategies through experiments based on the semiphysical testbed. We set $T = 250$ and the attack times $n = 10$ in the finite time horizon $[1, 250]$. It means that the attacker can assign the 10 times of attack in this period.

5.2. Simulation Results Analysis. We study the effectiveness of jamming attack with 10 different schedules when $R = 0$, $S_0 = S$, respectively (see Table 1). From Figure 3(a), we can compare the cost J under different attack schedules when $R = 0$. It can be seen that the attack schedule with 10 consecutive attack times can maximize the LQG cost. We also present the variation of system states and control data under optimal attack schedule in Figure 4. From this figure, these data will deviate the equilibrium points when the wireless channel is under jamming attack. Similarly, we can also study the LQG cost J under different attack schedules when $S_0 = S$. From Figure 3(b), we also can see that consecutive attack schedule is optimal. These experimental results can verify the theoretical conclusions in Section 4.

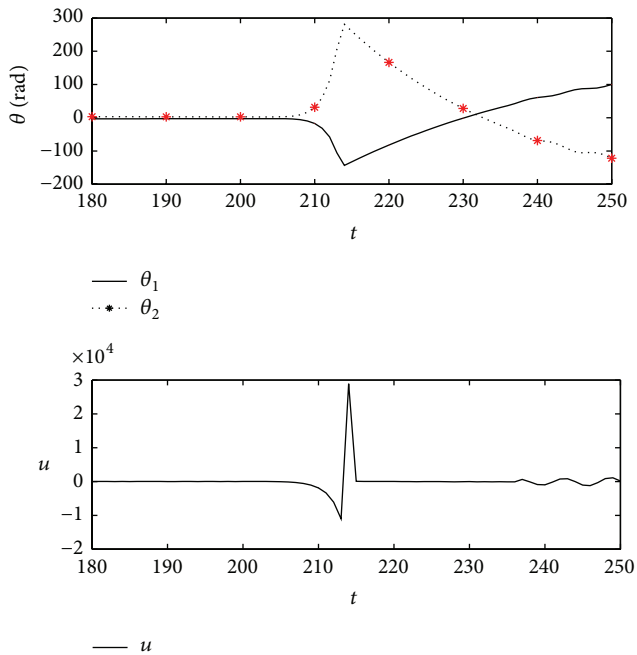


Figure 4: The variation of system states and control data under attack schedule 10 (optimal attack) when $R = 0$.

6. Conclusion

In this paper, we considered the optimal jamming attack scheduling which can destroy the system control performance. We formulated an optimization problem that maximizes the LQG cost subject to attacker's energy constraint in a given finite time horizon. Optimal attack schedule has been presented for two special cases. For the general case, we provided an algorithm to find the optimal attack schedule. We also established a semiphysical testbed and

studied the effectiveness of proposed attack schedules by simulation. In the future, we will study the evaluation of control performance when the NSCS is under other types of cyber attack, for example, data injection attack and replay attack. We will also design effective defense strategies to avoid the cyber attacks in NSCS.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The work was partially supported by Professional Development Program for Visiting Scholars in Colleges and Universities under Grant FX2014144 and Zhejiang Provincial Natural Science Foundation of China under Grant Y16F030011. The work by H. Zhang was supported by NSFC under Grants 61203036, 61503147, and 71401060, the University Science Research General Project of Jiangsu Province under Grant 15KJB510002, Huaihai Institute of Technology Doctoral Research Funding under Grant KQ15007, and Lianyungang Science and Technology Projects under Grants CK1331 and CN1321.

References

[1] R. A. Gupta and M.-Y. Chow, "Networked control system: overview and research trends," *IEEE Transactions on Industrial Electronics*, vol. 57, no. 7, pp. 2527–2535, 2010.

[2] S. He, J. Chen, D. K. Y. Yau, and Y. Sun, "Cross-layer optimization of correlated data gathering in wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 11, no. 11, pp. 1678–1691, 2012.

[3] L. Zhang, Y. Shi, T. Chen, and B. Huang, "A new method for stabilization of networked control systems with random delays," *IEEE Transactions on Automatic Control*, vol. 50, no. 8, pp. 1177–1181, 2005.

[4] S. He, J. Chen, F. Jiang, D. K. Y. Yau, G. Xing, and Y. Sun, "Energy provisioning in wireless rechargeable sensor networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 10, pp. 1931–1942, 2013.

[5] L. Schenato, B. Sinopoli, M. Franceschetti, K. Poolla, and S. S. Sastry, "Foundations of control and estimation over lossy networks," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 163–187, 2007.

[6] J. Chen, Q. Yu, P. Cheng, Y. Sun, Y. Fan, and X. Shen, "Game theoretical approach for channel allocation in wireless sensor and actuator networks," *IEEE Transactions on Automatic Control*, vol. 56, no. 10, pp. 2332–2344, 2011.

[7] Y. Zhang, S. He, J. Chen, Y. Sun, and X. Shen, "Distributed sampling rate control for rechargeable sensor nodes with limited battery capacity," *IEEE Transactions on Wireless Communications*, vol. 12, no. 6, pp. 3096–3106, 2013.

[8] S. He, X. Li, J. Chen, P. Cheng, Y. Sun, and D. Simplot-Ryl, "EMD: energy-efficient p2p message dissemination in delay-tolerant wireless sensor and actor networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 75–84, 2013.

[9] N. Bezzo, J. Weimer, M. Pajic, O. Sokolsky, G. J. Pappas, and I. Lee, "Attack resilient state estimation for autonomous robotic systems," in *Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS '14)*, pp. 3692–3698, Chicago, Ill, USA, September 2014.

[10] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, 2011.

[11] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *Hybrid Systems: Computation and Control*, vol. 5469 of *Lecture Notes in Computer Science*, pp. 31–45, Springer, Berlin, Germany, 2009.

[12] Y. Qi, P. Cheng, L. Shi, and J. Chen, "Event-based attack against remote state estimation," in *Proceedings of the IEEE Annual Conference on Decision and Control (CDC '15)*, Osaka, Japan, December 2015.

[13] F. Miao, M. Pajic, and G. J. Pappas, "Stochastic game approach for replay attack detection," in *Proceedings of the 52nd IEEE Conference on Decision and Control (CDC '13)*, pp. 1854–1859, IEEE, Firenze, Italy, December 2013.

[14] M. Zhu and S. Martínez, "On the performance analysis of resilient networked control systems under replay attacks," *IEEE Transactions on Automatic Control*, vol. 59, no. 3, pp. 804–808, 2014.

[15] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on SCADA systems," *IEEE Transactions on Control Systems Technology*, vol. 22, no. 4, pp. 1396–1407, 2014.

[16] J. He, P. Cheng, L. Shi, and J. Chen, "SATS: secure average-consensus-based time synchronization in wireless sensor networks," *IEEE Transactions on Signal Processing*, vol. 61, no. 24, pp. 6387–6400, 2013.

[17] R. Poisel, *Modern Communications Jamming Principles and Techniques*, Artech House, 2011.

[18] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal DoS attack policy against remote state estimation," in *Proceedings of the 52nd IEEE Conference on Decision and Control (CDC '13)*, pp. 5444–5449, Firenze, Italy, December 2013.

[19] A. Gupta, C. Langbort, and T. Başar, "Optimal control in the presence of an intelligent jammer with limited actions," in *Proceedings of the 49th IEEE Conference on Decision and Control (CDC '10)*, pp. 1096–1101, IEEE, Atlanta, Ga, USA, December 2010.

[20] H. Shisheh Foroush and S. Martinez, "On event-triggered control of linear systems under periodic denial-of-service jamming attacks," in *Proceedings of the 51st IEEE Conference on Decision and Control (CDC '12)*, pp. 2551–2556, IEEE, Maui, Hawaii, USA, December 2012.

[21] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal denial-of-service attack scheduling against linear quadratic gaussian control," in *Proceedings of the American Control Conference (ACC '14)*, pp. 3996–4001, Portland, Ore, USA, June 2014.

[22] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal denial-of-service attack scheduling with energy constraint," *IEEE Transactions on Automatic Control*, 2015.

[23] L. Shi, P. Cheng, and J. Chen, "Optimal periodic sensor scheduling with limited resources," *IEEE Transactions on Automatic Control*, vol. 56, no. 9, pp. 2190–2195, 2011.

[24] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal DoS attack scheduling in wireless networked control system," *IEEE Transactions on Control Systems Technology*, 2015.